This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

String

    - Webroot Software Spy Sweeper Enterprise Password Disclosure
    - WhitSoft Development SlimFTPd FTP Command Buffer Overflow
    - Youngzsoft CCProxy HTTP Request Processing Buffer Overflow
    - **Zinf Malformed Playlist File Remote Buffer Overflow (Updated)**
    - Zone Labs IMsecure Active Link Filter Bypass
- UNIX / Linux Operating Systems
    - **Apache mod_ssl SSLCipherSuite Access Validation (Updated)**
    - ARJ Software UNARJ Remote Buffer Overflow
    - **Carnegie Mellon University Cyrus SASL Buffer Overflow & Input Validation (Updated)**
    - Dave McMurtrie Up-IMAPProxy Multiple Remote Vulnerabilities
    - **FreeRADIUS Access-Request Denial of Service (Updated)**
    - **GD Graphics Library Remote Integer Overflow (Updated)**
    - **GNU GLibC Insecure Temporary File Creation (Updated)**
    - GNU JWhois Double Free Memory Corruption
    - GNU GNATS Format String
    - Heiko Stamer OpenSkat Weak Encryption Key Generation
    - **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
    - **Kaffeine Media Player Remote Buffer Overflow (Updated)**
    - **LibTIFF Buffer Overflows (Updated)**
    - Multiple Vendors GD Graphics Library Multiple Remote Buffer Overflows
    - Multiple Vendors Samba Remote Wild Card Denial of Service
    - Multiple Vendors EZ-IPupdate Remote Format String
    - Multiple Vendors Davfs2 Insecure Temporary File Creation
    - **Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows (Updated)**
    - Multiple Vendors MTink Insecure Temporary File Creation
    - Multiple Vendors Linux Kernel BINFMT_ELF

Loader Multiple Vulnerabilities

- - **Multiple Vendors Trustix LVM Utilities Insecure Temporary File Creation (Updated)**
  - **Multiple Vendors LibXpm Image Decoding Multiple Remote Buffer Overflow (Updated)**
  - **OpenSSL Insecure Temporary File Creation (Updated)**
  - PHPBB Remote URLDecode Input Validation
  - **Russell Marks ZGV Image Viewer Multiple Remote Integer Overflow (Updated)**
  - samhain sh_hash_compdata() Buffer Overflows
  - **Speedtouch USB Driver Format String (Updated)**
  - SQLgrey Postfix Greylisting Service SQL Injection
  - Sun One/IPlanet Messaging Server Webmail Hijack
  - Sun Java Runtime Environment InitialDirContext Remote Denial of Service
  - **Technote 'main.cgi' Input Validation (Updated)**
  - BNC Remote Buffer Overflow
  - BNC IRC Server Proxy Authentication Bypass
  - Thibault Godouet Fcron Multiple Vulnerabilities
  - Todd Miller Sudo Restricted Command Execution Bypass
  - TWiki Search Shell Metacharacter Remote Arbitrary Command Execution
  - **xmlsoft Libxml2 Multiple Remote Stack Buffer Overflows (Updated)**
  - **Yukihiro Matsumoto Ruby CGI Session Management Unsafe Temporary File (Updated)**
  - **Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service (Updated)**
- Multiple Operating Systems
  - Alcatel Speed Touch Pro With Firewall ADSL Router DNS Poisoning
  - Cisco IOS DHCP Input Queue Blocking Remote Denial of Service
  - Craig Knudsen WebCalendar Multiple Remote Vulnerabilities
  - David Djurback Chacmool Private Message System Multiple Vulnerabilities

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only		
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Nam
AlShare Software NetNote Server 2.2 (build 230)	A vulnerability exists which can be exploited by malicious people to cause a Denial of Service. The vulnerability is caused due to input validation errors when handling malformed traffic. No workaround or patch available at time of publishing. An exploit script has been published.	NetNote Serve Remote Denia of Service
Cisco Cisco Security Agent (CSA) prior to 4.0.3 build 728	A vulnerability exists that could allow a remote malicious user to conduct buffer overflow attacks against the target system that will not be detected by CSA. The vendor reported that a properly timed attack can evade the CSA attack detection mechanism, where the second of two buffer overflow attacks will not be detected. An authenticated user must be logged in or the hidden GUI option must be in effect for the attack to be	Cisco Security Agent Speciall Timed Buffer Overflow

	successful. Update to version 4.0.3 build 728 available at: www.cisco.com/warp/public/707/cisco-sa-20041111-csa.shtml Currently we are not aware of any exploits for this vulnerability.	
Clearswift MIMEsweeper for SMTP 5.x	A vulnerability exists which potentially can be exploited by malware to bypass the scanning functionality. The problem is that emails containing encrypted data (e.g. password-protected zip files) erroneously are marked as 'Clean' instead of 'Encrypted.' The vulnerability only affects versions that have been upgraded from: * MAILsweeper Business Suite I * MAILsweeper Business Suite II * MAILsweeper for SMTP version 4.3 Apply hotfix: http://www.clearswift.com/download/info.aspx?ID=552 Currently we are not aware of any exploits for this vulnerability.	Clearswift MIMEsweepe for SMTP Encrypted Emails Misclassificatio
Google Google Desktop Search	A remote malicious user can create a specially crafted URL that, when loaded by a target user that has Google Desktop Search installed, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the Google site and will run in the security context of that site. **The vendor has issued a fix.** A Proof of Concept exploit has been published.	Google Deskto Search Input Validation
IceWarp Merak Mail Server 7.5.2 and 7.6.0 with Icewarp Web Mail	Multiple vulnerabilities exist in Merak Mail Server with IceWarp Web Mail. A remote malicious user can conduct Cross-Site Scripting attacks and a remote authenticated user can rename and delete files on the target system. Among other errors, several scripts do not properly validate user-supplied input, including send.html, attachment.html, and folderitem.html. **Upgrades available at: http://www.icewarp.com/Download/** A Proof of Concept exploit has been published.	IceWarp Mera Mail Server Multiple Remot Vulnerabilities
Infuseum Infuseum's ASP Message Board (AMB)	Multiple input validation vulnerabilities exists that could permit a remote malicious user to inject SQL commands and conduct Cross-Site Scripting attacks. A remote user can supply specially crafted input to execute SQL commands on the underlying database. A remote user can also cause arbitrary	Infuseum Inpu Validation Vulnerabilities

2.2.1c	scripting code to be executed by the target user's browser. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	
Ipswitch IMail 8.13	A buffer overflow vulnerability exists in the 'DELETE' command due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Ipswitch IMail Server Remot Buffer Overflo
Kerio Technologies Inc. Kerio Personal Firewall 4.1.2 and prior	A vulnerability exists that could permit a remote malicious user to cause Denial of Service conditions. There is a packet processing flaw that can trigger 100% CPU utilization on the target system. The vendor has issued a fixed version (4.1.2), available at: http://www.kerio.com/kpf_download.html **An exploit script has been published**	Kerio Persona Firewall Remot Denial of Service
Microsoft Internet Explorer 6.0	A vulnerability exists that can be exploited by malicious sites to detect the presence of local files. This is because an 'Access is Denied' error will be returned if a site in the 'Internet' zone tries to open an existing local file in the search window using the 'res:' URI handler. This can be exploited to determine the presence of specific programs or files in the system directories and on the desktop. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Microsoft Internet Explorer 'res:' URI Handler File Identification
Microsoft ISA Server 2000, Proxy Server 2.0	A spoofing vulnerability exists that could enable a malicious user to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious website. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms04-039.mspx **V2.0 (November 9, 2004): Bulletin updated to reflect the release of an updated ISA Server 2000 security update for the German language only. This issue does not affect any other language version of this security update. The Security Update Replacement section has also been revised.**	Microsoft Server Spoofin CVE Name: CAN-2004-089

	V3.0 (November 16, 2004): Bulletin updated to reflect the release of updated ISA Server 2000 security updates for all languages. These issues affected customers using ISA Server 2000 Service Pack 1 or using Windows 2000 Service Pack 3. The Security Update Replacement section has also been revised. Currently we are not aware of any exploits for this vulnerability.	
Microsoft Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6.0 for Windows Server 2003, Internet Explorer 6.0 for Windows XP Service Pack 2, Windows 98, Windows 98 SE, Windows ME, Internet Explorer 5.5; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server, S8100 Media Servers	Multiple vulnerabilities are corrected with Microsoft Security Update MS04-038. These vulnerabilities include: Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability; Similar Method Name Redirection Cross Domain Vulnerability; Install Engine Vulnerability; Drag and Drop Vulnerability; Address Bar Spoofing on Double Byte Character Set Locale Vulnerability; Plug-in Navigation Address Bar Spoofing Vulnerability; Script in Image Tag File Download Vulnerability; SSL Caching Vulnerability. These vulnerabilities could allow remote code execution. A vulnerability exists in the Microsoft MSN 'heartbeat.ocx' component, used by Internet Explorer on some MSN gaming sites Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() **Updated the ActiveX control name from "Heartbeat.ocx" to "Hrtbeat.ocx", added GUID information to the Security Update Information section.** Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Security Updat CVE Names: CAN-2004-084 CAN-2004-072 CAN-2004-021 CAN-2004-083 CAN-2004-084 CAN-2004-084 CAN-2004-084 CAN-2004-084
Microsoft	A vulnerability exists which can be exploited by malicious	Internet

Internet Explorer 6, Microsoft Outlook Express 6	people to trick users into visiting a malicious website by obfuscating URLs. This vulnerability was confirmed in SP1 but not SP2. Update to Windows XP SP2. Proofs of Concept exploit scripts have been published.	Explorer Flash Content Status Bar Spoofing
Microsoft Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, XP Home, SP1&SP2, XP Professional, SP1&SP2	A buffer overflow vulnerability exists in the 'ddeshare.exe' utility, which could possibly let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows DDEShare Buffer Overflow
Microsoft Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003	A remote code execution vulnerability exists in the Windows Server 2003 SMTP component due to the way Domain Name System (DNS) lookups are handled. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx **Bulletin updated to clarify restart requirement for Windows Server 2003 and Windows XP 64-Bit.** Currently we are not aware of any exploits for this vulnerability.	Microsoft SMT Remote Code Execution CVE Name: CAN-2004-084

New Media Generation Hired Team: Trial 2.0 / 2.200 & prior	Several vulnerabilities exist: a format string vulnerability exists when a remote malicious user joins a game and then submits a specially crafted message, which could cause a Denial of Service or potentially the execution of arbitrary code; a vulnerability exists when a remote malicious user submits data to one of the server-assigned UDP ports that causes the match to be interrupted; a remote Denial of Service vulnerability exists when the statue command is invoked; and several flaws exist in the Shine engine (which is which the game is based on). No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Hired Team: Trial Format String
PacketCell Networks Hotfoon 4.0	A vulnerability exists that could allow a remote malicious user on the Hotfoon chat feature to send an arbitrary URL to the target user to cause the target user's Hotfoon application to open the link without first asking or alerting the target user. No solution is available at this time. A Proof of Concept exploit has been published.	Hotfoon Diale Chat Open Arbitrary URL
Protection Technology StarForce Professional 3.0	A vulnerability exists in the drivers that may permit a local user to obtain elevated privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Protection Technology StarForce Professional Elevated Privileges
Robert K Jung unarj 2.x	An input validation vulnerability was reported in unarj, which could permit a remote user to create a malicious archive that, when expanded by a target user, will write or overwrite arbitrary files on the target user's system. **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** A Proof of Concept exploit has been published.	Unarj Input Validation
SecureAction Research Secure Network Messenger 1.4.2 and prior versions	A vulnerability exists which could permit a remote user to cause the application to crash. A remote user can connect to the target system on port 6144 and send 10 or more carriage return characters, then disconnect, then connect again and send a carriage return to cause the target service to crash. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	SecureAction Research Secure Networ Messenger Denial of Service

Skype Technologies Skype for Windows 1.0.*.95 through 1.0.*.98	A vulnerability exists which can be exploited by malicious people to execute arbitrary code. The vulnerability is caused due to a boundary error within the handling of command line arguments. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into visiting a malicious web site, which passes an overly long string (more than 4096 bytes) to the 'callto:' URI handler. Update to version 1.0.0.100: http://www.skype.com/products/skype/windows/ Currently we are not aware of any exploits for this vulnerability.	Skype 'callto:' URI Handler Buffer Overflo
Soft3304 04WebServer 1.42	Multiple vulnerabilities exist that could allow a remote malicious user to inject arbitrary characters into the log file, conduct Cross-Site Scripting attacks, or cause a Denial of Service. The default 404 Not Found response (Response_default.html) does not properly filter HTML code before displaying the originally requested URL. A remote malicious user can also inject arbitrary characters into the log file or request a MS-DOS device name to prevent the server from restarting properly. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Soft3304 04WebServe Input Validatio Vulnerabilitie
The 3DO Company Army Men RTS 1.x	A format string vulnerability exists which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Army Men RT Format String
Webroot Software Spy Sweeper Enterprise 1.5.1.3698	A vulnerability exists that can be exploited by malicious, local users to disclose sensitive information. The problem is that the administrative password used for overriding settings from client systems is stored in clear text in a location in the registry, which is readable by all users. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Spy Sweeper Enterprise Password Disclosure
WhitSoft Development SlimFTPd 3.15 and prior	A buffer overflow vulnerability exists in SlimFTPd which could allow a remote authenticated malicious user to execute arbitrary code on the target system. A remote authenticated user, including an anonymous user, can supply a specially crafted command (e.g., CWD, STOR, MKD, STAT) to trigger a buffer overflow. The vendor has issued a fixed version (3.16), available at:	WhitSoft Development SlimFTPd FT Command Buffer Overflo

	http://www.whitsoftdev.com/files/slimftpd.zip An exploit script has been published.	
YoungZsoft CCProxy 6.0	A vulnerability exists which could allow the execution of arbitrary code. The vulnerability is caused due to a boundary error within the handling of HTTP requests. This can be exploited to cause a buffer overflow by sending an overly long HTTP GET request. Update to version 6.2: http://www.youngzsoft.net/ccproxy/ An exploit script has been published.	CCProxy HTT Request Processing Buffer Overflo
Zinf Zinf 2.2.1	A buffer overflow vulnerability exists when processing malformed playlist files, which could let a remote malicious user obtain unauthorized access. **Debian: http://security.debian.org/pool/updates/main/f/freeamp/** An exploit script has been published.	Zinf Malforme Playlist File Remote Buffe Overflow CVE Name: CAN-2004-096
Zone Labs IMsecure and IMsecure Pro prior to 1.5	A vulnerability exists which can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a canonicalization error in the Active Link filter, which blocks URLs in IM messages. This can be exploited to bypass the filter by using encoded representations for various characters. Update to version 1.5 or later: http://www.zonelabs.com/store/content/home.jsp Currently we are not aware of any exploits for this vulnerability.	Zone Labs IMsecure Activ Link Filter Bypass

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common
Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo:	Apache m SSLCiph Access Va CVE N CAN-200

	http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesoft.com/security/advisories **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-562.html** There is no exploit code required.	
ARJ Software Inc. UNARJ 2.62-2.65	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied strings prior to processing, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/	ARJ Sof UNARJ R Buffer O CVE N CAN-200

	Currently we are not aware of any exploits for this vulnerability.	
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-sasl/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus SAS Overflow Valida CVE N CAN-200
Dave McMurtrie up-imapproxy, 1.2.2	Multiple vulnerabilities exist: several remote Denial of Service vulnerabilities exist due to the way literal values are processed; and a vulnerability exists because literal value sizes are stored in signed integer format, which could let a remote malicious user on 64-bit systems obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Up-IMAF Multiple F Vulneral
FreeRADIUS Server Project FreeRADIUS 0.2-0.5, 0.8, 0.8.1, 0.9-0.9.3. 1.0	A remote Denial of Service vulnerability exists in 'radius.c' and 'eap_tls.c' due to a failure to handle malformed packets. Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-29.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-609.html**	FreeRA Access-R Denial of CVE Na CAN-200 CAN-200 CAN-200

	There is no exploit code required.	
GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml **Debian:** **http://security.debian.org/pool/updates/main/libg** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** An exploit script has been published.	GD Gra Library R Integer O CVE N CAN-200
GNU glibc 2.0-	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files.	GN GLibC In Tempora

2.0.6, 2.1, 2.1.1 -6, 2.1.1, 2.1.2, 2.1.3 -10, 2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3-2.3.4, 2.3.10	Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/glibc/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** There is no exploit code required.	Creat CVE N CAN-200
GNU jwhois 3.2.2	A double free vulnerability exists when an attempt is made to process whois requests that result in more than one redirection, which could possibly let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Currently we are not aware of any exploits for this vulnerability.	JWhois I Free Me Corrup
GNU GNATS 3.0 02, 3.2, 3.14 b, 3.113 .1_6, 3.113, 3.113.1, 4.0	A format string vulnerability exists in 'misc.c,' which could let a malicious user execute arbitrary code. **Debian:** **http://security.debian.org/pool/updates/main/g/gnats/** Currently we are not aware of any exploits for this vulnerability.	GNU Gl Format
Heiko Stamer OpenSkat 1.1-1.9, 2.0	A weak encryption key generation vulnerability exists due to a design error, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://freshmeat.net/redir/openskat/36295/url_tgz/openSkat-2.1.tar.gz	Heiko S OpenSka Encryptic Genera

	Currently we are not aware of any exploits for this vulnerability.	
Info-ZIP Zip 2.3	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml** Currently we are not aware of any exploits for this vulnerability.	Info-ZI Remote R Direct Compre Buffer O CVE N CAN-200
Kaffeine Media Player 0.4.2, 0.4.3 b, 0.4.3, 0.5 rc1	A buffer overflow vulnerability exists in the processing of Content-Type headers in the 'http_open()' function in 'http.c' due to insufficient boundary checks on user-supplied strings prior to copying them into finite stack-based buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-14.xml** A Proof of Concept exploit has been published.	Kaffeine Player R Buffer O
libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo:	LibTIFF Overfl CVE N CAN-200 CAN-200 CAN-200

http://security.gentoo.org/glsa/glsa-200410-11.xml

Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/

OpenPKG:
ftp://ftp.openpkg.org/release/

Trustix: ftp://ftp.trustix.org/pub/trustix/updates/

Mandrake: http://www.mandrakesecure.net/en/ftp.php

SuSE: ftp://ftp.suse.com/pub/suse/

RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html

Slackware:
ftp://ftp.slackware.com/pub/slackware/

Conectiva: ftp://atualizacoes.conectiva.com.br/

Proofs of Concept exploits have been published.

Multiple Vendors GD Graphics Library gdlib 1.8.4, 2.0.1, 2.0.20-2.0.23, 2.0.26-2.0.28	Multiple buffer overflow vulnerabilities exist due to insufficient bounds checking prior to processing user-supplied strings, which could let ak remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Currently we are not aware of any exploits for these vulnerabilities.	GD Gra Library M Remote Overfl CVE N CAN-200
Multiple Vendors Gentoo Linux; Samba Samba 3.0-3.0.7	A remote Denial of Service vulnerability exists in 'ms_fnmatch()' function due to insufficient input validation. Patch available at: http://us4.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch Gentoo: http://security.gentoo.org/glsa/glsa-200411-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/samba/ There is no exploit code required.	Samba F Wild Card Serv CVE N CAN-200
Multiple Vendors Angus Mackay ez-ipupdate 3.0.11 b8, 3.0.11 b5; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips,	A format string vulnerability exists in the 'show_message()' function, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/e/ez-ipupdate/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php	EZ-IPu Remote I Strir CVE N CAN-200

m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux	SuSE: http://www.suse.de/en/private/download/updates/92_i386.html Currently we are not aware of any exploits for this vulnerability.	
Multiple Vendors Davfs Davfs2 0.2 .0-0.2.2; Gentoo Linux	A vulnerability exists in WEB-DAV Linux File System (dav2fs) because temporary .pid files are creates insecurely, which could let a malicious user obtain elevated privileges. Davfs: http://prdownloads.sourceforge.net/dav/davfs2-0.2.3.tar.gz?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-22.xml There is no exploit code required.	Davfs2 Ir Tempora Creat

Multiple Vendors
 	
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;
 	
Gentoo Linux;
 	
GNOME GPdf 0.112;
KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2;
RedHat Fedora Core2;
	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.
	
	Debian:
	http://security.debian.org/pool/updates/main/c/cupsys/
	
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	
	Gentoo: http://security.gentoo.org/glsa/glsa-200410-20.xml
	
	KDE:
	ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff
	
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/
	
	Conectiva: ftp://atualizacoes.conectiva.com.br/
	
	Currently we are not aware of any exploits for these vulnerabilities.
		Xpdf PDI
		Multiple I
		Overfl
		
		CVE Na
		CAN-200
		CAN-200

Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0		
Multiple Vendors Gentoo Linux; Jean-Jacques Sarton mtink 0.9.32, 0.9.33, 0.9.53, 1.0.4	A vulnerability exists due a failure to verify the existence of a file before writing to it, which could let a malicious user overwrite arbitrary files with the privileges of the user running the utility. Upgrades available at: http://xwtools.automatix.de/files/mtink-1.0.5.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200411-17.xml There is no exploit code required.	MTink In Tempora Creat
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/linux-2.6/gnupatch@41925edcVccsXZXObG444GFvEJ94GQ Proofs of Concept exploit scripts have been published.	Linux K BINFMT Loader M Vulnerab
Multiple Vendors LVM Logical Volume Management Utilities 1.0.4, 1.0.7, 1.0.8	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lvm10/ Debian: http://security.debian.org/pool/updates/main/l/lvm10/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-22.xml** There is no exploit code required.	Trustix Utilities In Tempora Creat CVE N CAN-200

Multiple Vendors OpenBSD 3.4, 3.5; SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8; X.org X11R6 6.7.0, 6.8; XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0; Avaya Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	Multiple vulnerabilities exist: a stack overflow vulnerability exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in -create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ SuSE: ftp://ftp.suse.com/pub/suse/ X.org: http://x.org/X11R6.8.1/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-34.xml IBM: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203389& PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57652-1&searchclause= Mandrake: http://www.mandrakesoft.com/security/advisories **HP: http://www.itrc.hp.com/service/patch/mainPage.do**	LibXpm Decoding Remote Overf CVE Na CAN-200 CAN-200

	Proofs of Concept exploits have been published.	
OpenSSL Project OpenSSL 0.9.6, 0.9.6 a-0.9.6 m, 0.9.7c	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-15.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/o/openssl/** There is no exploit code required.	Open Insec Tempora Creat CVE N CAN-200
phpBB Group phpBB 2.0.0-2.0.10	A vulnerability exists in the 'urldecode' function due to insufficient input validation, which could let a remote malicious user execute arbitrary PHP script. No workaround or patch available at time of publishing. There is no exploit code required.	PHPBB F URLDeco Valida
Russell Marks zgv Image Viewer 5.5	Several vulnerabilities exist due to various integer overflows when processing images, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-12.xml** Currently we are not aware of any exploits for these vulnerabilities.	ZGV Imag Multiple F Integer O
Samhain Labs Samhain 1.8.9, 2.0.1	Several vulnerabilities exist: a buffer overflow vulnerability exists when in 'update' mode in the 'sh_hash_compdata()' function, which could let a malicious user execute arbitrary code; and a vulnerability exists in the 'sh_hash_compdata()' function due to a potential null pointer dereference, which could let a malicious user execute arbitrary code. Upgrades available at: http://la-samhna.de/samhain/samhain-current.tar.gz	samh sh_hash_c () Buffer O

	Currently we are not aware of any exploits for these vulnerabilities.	
Speedtouch USB Driver 1.0, 1.1, 1.2 , beta1-beta3, 1.3	A format string vulnerability exists because the 'modem_run,' 'pppoa2,' and 'pppoa3' functions make an unsafe 'syslog()' call due to insufficient sanitization, which could let a malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=32758&package_id=28264&release_id=271734 Gentoo: http://security.gentoo.org/glsa/glsa-200411-04.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Speedtou Driver F Strir CVE N CAN-200
SQLgrey Postfix Greylisting Service 1.1.1, 1.1.3	A vulnerability exists due to insufficient sanitization of sender and recipient emails before being used in a SQL query, which could let a remote malicious user manipulate SQL queries. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=113566 There is no exploit code required.	SQLgrey Greylisting SQL Inj
Sun Microsystems, Inc. iPlanet Messaging Server 5.2; Sun ONE Messaging Server 6.1	A vulnerability exists in the webmail functionality when processing emails, which could let a remote malicious user obtain unauthorized access. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57665-1 Currently we are not aware of any exploits for this vulnerability.	Sun One/ Messagin Webmail
Sun Microsystems, Inc. Java 2 Runtime Environment 1.4.2, 1.5	A remote Denial of Service vulnerability exists in the 'InitialDirContext' environment variable due to a failure to keep track of DNS requests. No workaround or patch available at time of publishing. There is no exploit code required.	Sun Java Enviror InitialDirC Remote D Serv
Technote	A vulnerability exists in the 'main.cgi' script due to insufficient	Technote '

Technote	validation of user-supplied input in the 'filename' parameter, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. **An exploit script has been published.**	Input Val
The BNC Project BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2, 2.8.8, 2.8.9	A buffer overflow vulnerability exists in ' getnickuserhost' when a malformed IRC server response is handled by the proxy, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.gotbnc.com/files/bnc2.9.1.tar.gz Currently we are not aware of any exploits for this vulnerability.	BNC Re Buffer O
The BNC Project BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2, 2.8.8, 2.8.9, 2.9 .0	A vulnerability exists due to code modifications after the recent release (BNC 2.9.0), which could let a malicious user bypass authentication. Upgrades available at: http://www.gotbnc.com/files/bnc2.9.1.tar.gz There is no exploit code required.	BNC IRC Pro Authenti Bypa
Thibault Godouet Fcron 2.x	Multiple vulnerabilities exist: a vulnerability exists in the 'fcronsighup' utility due to a design error, which could let a malicious user obtain sensitive information; a vulnerability exists because the 'fcronsighup' utility can bypass access restrictions, which could let a malicious user supply arbitrary configuration settings; an input validation vulnerability exists in the 'fcronsighup' utility, which could let a malicious user delete arbitrary files; and a vulnerability exists because a malicious user can view the contents of the 'fcron.allow' and 'fcron.deny' files due to a file descriptor leak. Update available at: http://fcron.free.fr/download.php Currently we are not aware of any exploits for these vulnerabilities.	Thibault G Fcron M Vulnera CVE Na CAN-200 CAN-200 CAN-200 CAN-200
Todd Miller Sudo 1.5.6-1.5.9, 1.6-1.6.8	A vulnerability exists due to an error in the environment cleaning, which could let a malicious user execute arbitrary commands. Patch available at: http://www.courtesan.com/sudo/download.html There is no exploit code required.	Sudo Re Comm Execution
TWiki	A vulnerability exists in 'Search.pn' due to an input validation error	TWiki Sea

TWiki 20030201	when handling search requests, which could let a remote malicious user execute arbitrary commands. Hotfix available at: http://twiki.org/cgi-bin/view/Codev/SecurityAlert Execute CommandsWithSearch There is no exploit code required; however, a Proof of Concept exploit has been published.	Metacha Remote A Comm Execu
xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy ()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-05.xml Mandrake: http://www.mandrakesoft.com/security/advisories OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: http://www.trustix.org/errata/2004/0055/ Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/libx/libxml2/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-615.html** An exploit script has been published.	Libxml2 M Remote Buffer Ov CVE N CAN-200

Yukihiro Matsumoto Ruby 1.6, 1.8	A vulnerability exists in the CGI session management component due to the way temporary files are processed, which could let a malicious user obtain elevated privileges. Upgrades available at: http://security.debian.org/pool/updates/main/r/ruby/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-08.xml RedHat: http://rhn.redhat.com/errata/RHSA-2004-441.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Ruby CGI Manage Unsafe Te Fil CVE N CAN-200

Yukihiro Matsumoto Ruby 1.8.x	A remote Denial of Service vulnerability exists due to an input validation error in 'cgi.rb.' Debian: http://security.debian.org/pool/updates/main/r/ruby Mandrake: http://www.mandrakesoft.com/security/advisories **Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/l** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Ruby Infin Remote D Serv CVE N CAN-200

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Nam
Alcatel SpeedTouch Pro With Firewall ADSL Router	A DNS poisoning vulnerability exists, which could let a remote malicious user spoof addresses, carry out man-in-the-middle attacks, and trigger potential Denial of Service conditions. No workaround or patch available at time of publishing. An exploit script is not required.	Alcatel Speed Touch Pro Wit Firewall ADSL Router DNS Poisoning
Cisco Systems, 2650 Multiservice Platform, 2650XM Multiservice Platform, 2651 Multiservice Platform, 2651XM Multiservice Platform, Cisco 7200, 7300, 7500, 7600, Catalyst 7600	A remote Denial of Service vulnerability exists when a malicious user submits specially crafted DHCP packets that will remain in the queue. Updates and workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml An exploit script is not required.	Cisco IOS DHC Input Queue Blocking Remo Denial of Servic

Sup720/MSFC3, IOS 12.2 (18)SW, 12.2 (18)SV, 12.2 (18)SE, 12.2 (18)S,12.2 (18)EWA, 12.2 (18)EW, 12.2 (14)SZ		
Craig Knudsen WebCalendar 0.9.8, 0.9.11, 0.9.15, 0.9.16, 0.9.19-0.9.44	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input passed to some parameters in various scripts, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'login.php' because input passed to the 'return_path' parameter can inject malicious characters into HTTP headers, which could let a remote malicious user execute arbitrary HTML and script code and perform web cache poisoning; a vulnerability exists in 'init.php' due to insufficient verification of input passed to the 'user_inc' parameter, which could let a remote malicious user include arbitrary files from local resources; a vulnerability exists in 'upcoming.php' because some internal variables in 'view_entry.php' can be overwritten by external parameters, which could let a remote malicious user bypass security restrictions; and a vulnerability exists in 'validate.php' when accessed with an empty 'encoded_login' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Craig Knudsen WebCalendar Multiple Remot Vulnerabilities
David Djurback chacmool Private Message System 1.1.3	Several vulnerabilities exist in the Private Messaging System (PMS) 3rd party add-on for punBB, which could let a remote malicious user obtain sensitive information and execute arbitrary code. No workaround or patch available at time of publishing. An exploit script is not required; however, a	David Djurback Chacmool Priva Message Syste Multiple Vulnerabilities

	Proof of Concept exploit has been published.	
DUware DUgallery	A vulnerability exists which could let a remote malicious user download the database and obtain the administrative password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	DUgallery Database Disclosure
forum-aztek.com Aztek Forum 4.0	Cross-Site Scripting vulnerabilities exist in 'forum_2.php' in the 'return' and 'title' variables, in the 'search' parameter in 'search.php,' and the 'email' parameter in 'subscribe.php' due to insufficient input sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. An exploit script is not required; however, a Proof of Concept exploit has been published.	Aztek Forum Multiple Cross Site Scripting
Mantis Mantis prior to 0.19.1	Several vulnerabilities exist: a vulnerability exists in the 'All Projects' summary, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because it is possible to monitor filed bugs even when you have been removed from the project, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/showfiles.php?group_id=14963 There is no exploit code required.	Mantis Access Control Information Disclosure
Mark Zuckerberg Thefacebook	Multiple Cross-Site Scripting vulnerabilities exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. An exploit script is not required; however, Proofs of Concept exploits have been published.	Mark Zuckerbe Thefacebook Multiple Cross Site Scripting
miniBB.net	A vulnerability exists in the 'index.php' script due	miniBB 'user'

miniBB prior to 1.7f	to insufficient validation of the 'user' parameter, which could let a remote malicious user obtain sensitive information. Update available at: http://www.minibb.net/index.php?p=download A Proof of Concept exploit has been published.	Parameter Inpu Validation
Mozilla,.org Firefox 0.8, 0.9-0.9.3, 0.10, 0.10.1	Multiple vulnerabilities exist: a vulnerability exists because web sites may include images from local resources, which could let a malicious user obtain sensitive information, cause a Denial of Service, and potentially steal passwords from Windows systems; a vulnerability exists in the file download dialog box because filenames are truncated, which could let a malicious user spoof downloaded file names; and a vulnerability exists on MacOSx because Firefox is installed with world-writable permissions, which could let a malicious user obtain elevated privileges. Upgrades available at: http://www.mozilla.org/products/firefox/ An exploit script is not required	Mozilla Firefox Multiple Vulnerabilities
Multiple Vendors Archive::Zip 1.13, F-Secure Anti-Virus for Microsoft Exchange 6.30, 6.30 SR1, and 6.31, Computer Associates, Eset, Kaspersky, McAfee, Sophos, RAV	Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows malicious users to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. Instructions for Computer Associates, Eset, Kaspersky, McAfee, Sophos, and RAV are available at: http://www.idefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true Gentoo: http://security.gentoo.org/glsa/glsa-200410-31.xml Mandrakelinux 10.1 and Mandrakelinux 10.1/X86_64: http://www.mandrakesoft.com/security/advisories	Multiple Vendc Anti-Virus Software Detection Evasi CVE Names: CAN-2004-093 CAN-2004-093 CAN-2004-093 CAN-2004-093 CAN-2004-093 CAN-2004-093

	A fix for F-Secure is available at:: ftp://ftp.f-secure.com/support/hotfix/fsav-mse/fsavmse63x-02.zip Proofs of Concept exploits have been published.	

Multiple Vendors
 	
Axis Communications 2100 Network Camera 2.0-2.03, 2.12, 2.30-2.34, 2.40, 2.41, 2110 Network Camera 2.12, 2.30-2.32, 2.34, 2.40, 2.41, 2120 Network Camera 2.12, 2.30-2.32, 2.34, 2.40, 2.41, 2400+ Video Server 3.11, 3.12, 2401 Video Server 3.12, 2420 Network Camera 2.12, 2.30-2.34, 2.40, 2.41, 2460 Digital Video Recorder 3.12;
dnrd dnrd 1.0-1.4, 2.0-2.10; Don Moore MyDNS 0.6 ,x, 0.7 ,x, 0.8 ,x, 0.9 ,x 0.10 .0;
Posadis Posadis m5pre1&2, 0.50.4-0.50.9, 0.60 .0, 0.60.1
	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted DNS response that contains a spoofed source address.
	
	Axis:
	http://www.axis.com/techsup/firmware.php
	
	DNRD:
	http://prdownloads.sourceforge.net/dnrd/dnrd-2.17.1.tar.gz?download
	
	Don Moore:
	http://mydns.bboy.net/download/mydns-0.11.0.tar.gz
	
	Posadis:
	http://prdownloads.sourceforge.net/posadis/
	
	Currently we are not aware of any exploits for this vulnerability.
		Multiple Vendo
		DNS Remote
		Denial of Servic
		
		CVE Name:
		CAN-2004-078

Multiple Vendors
 	
Eudora Qpopper 3.1.2;
Ipswitch IMail 6.0.6;
ProFTPD Project ProFTPD 1.2-1.2.9; RhinoSoft Serv-U 3.0;
Washington University wu-ftpd 2.4.1, 2.4.2 VR17, 2.4.2 VR16, 2.5 .0, 2.6.0-2.6.2
	A vulnerability exists due to a server response splitting weakness, which could let a remote malicious user have attacker-specified data echoed back to the computer that the request originated from.
	
	No workaround or patch available at time of publishing.
	
	An exploit script is not required.
		Multiple Vendo
		Server Respons
		Filtering

Multiple Vendors Gentoo Linux; Pavuk Pavuk 0.9pl28i, 0.928 r1&r2, 0.9 pl30b, 0.9 pl28	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the digest authentication handler due to some boundary errors which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists when processing HTTP header information, which could let a remote malicious user execute arbitrary code; and several buffer	Pavuk Multiple Remote Buffe Overflows CVE Name: CAN-2004-045

	overflow vulnerabilities exists due to unspecified boundary errors, which could let a remote malicious user execute arbitrary code. Update available at: http://sourceforge.net/project/showfiles.php?group_id=81012 Gentoo: http://security.gentoo.org/glsa/glsa-200411-19.xml Currently we are not aware of any exploits for these vulnerabilities.	
Multiple Vendors Microsoft Internet Explorer 6.0, SP1&SP2; Mozilla Firefox 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, Netscape 7.0	Multiple vulnerabilities exist in the image handling functionality through the <IMG> tag, which could let a remote malicious user cause a Denial of Service, and obtain sensitive information. Mozilla: http://www.mozilla.org/products/firefox/ A Proof of Concept exploit has been published.	Multiple Browse IMG Tag Multip Vulnerabilities
Netgear DG834 ADSL Firewall Router	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists due to an error in the connection handling for the administrative web interface; and a vulnerability exists in the content filtering functionality, which could let a remote malicious user bypass access restrictions. No workaround or patch available at time of publishing. There is no exploit code required.	Netgear DG83 ADSL Firewal Router Multipl Vulnerabilities
Nucleus CMS Nucleus CMS 3.1	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to insufficient sanitization of user-supplied input before being used in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for	Nucleus CMS Multiple Input Validation

	these vulnerabilities.	
nuked-klan.org NuKed-KlaN	A Cross-Site Scripting vulnerability exists due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	NuKed-KlaN Cross-Site Scripting
Pablo Hernandez GFHost 0.2	Multiple Cross-Site Scripting vulnerabilities exist in the 'label.php' and 'dl.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. An exploit script is not required; however, Proofs of Concept exploits have been published.	Pablo Hernande GFHost Cross Site Scripting & Server-Side Scr Execution
paystream. sourceforge.net AudienceConnect RemoteEditor prior to 0.1.6	A vulnerability exists in the IP address-access control feature, which could let a remote malicious user obtain unauthorized access. Update available at: http://sourceforge.net/project/showfiles.php?group_id=98629&package_id=132533 Currently we are not aware of any exploits for this vulnerability.	AudienceConne RemoteEditor Unauthorized Access
paystream. sourceforge.net AudienceConnect RemoteEditor prior to 0.1.1	A vulnerability exists when a remote malicious user submits a form with content that exceeds the CONTENT_MAX value. The impact was not specified. Update available at: http://sourceforge.net/project/showfiles.php?group_id=98629&package_id=132533 Currently we are not aware of any exploits for this vulnerability.	AudienceConne RemoteEditor Oversized Submission
Phorum Phorum 5.0.3 BETA, 5.0.7 BETA, 5.0.9-5.0.12	An input validation vulnerability exists in 'follow.php' due to insufficient validation of user-supplied input in the 'forum_id' parameter, which could let a remote malicious user execute arbitrary SQL commands.	Phorum 'follow.php' Inpu Validation

	Upgrades available at: http://phorum.org/downloads/phorum-5.0.13.tar.gz A Proof of Concept exploit script has been published.	
phpWebSite Development Team phpWebsite 0.7.3, 0.8.2, 0.8.3, 0.9.3, -1-4	A vulnerability exists in the 'index.php' script due to insufficient validation of user-supplied input in several parameters, which could let a remote malicious user execute arbitrary HTML and script code. Patches available at: http://phpwebsite.appstate.edu/downloads/security/phpwebsite-core-security-patch2.tar.gz An exploit script is not required; however, a Proof of Concept exploit has been published.	phpWebSite HTTP Respons Splitting
powerportal.sourceforge.net PowerPortal 1.3	A vulnerability exists in the 'index.php' script due to insufficient validation of the 'index_page' variable, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PowerPortal 'index_page' Inp Validation
PvPGN PvPGN 1.6.0-1.6.6	A buffer overflow vulnerability exists due to insufficient boundary checks performed on 'gamereport' packets, which could let a remote malicious user execute arbitrary code. Update available at: http://pvpgn.berlios.de/index.php?page=files Currently we are not aware of any exploits for this vulnerability.	PvPGN GameReport Packet Handle Remote Buffe Overflow
Salims Softhouse JAF CMS 1.0, 1.5, 2.0, 2.0.5, 2.1 .0, 2.5, 3.0 RC	A Directory Traversal vulnerability exists in 'config.php' due to insufficient input validation of the 'show' parameter, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/showfiles.php?group_id=113192&package_id=122433&release_id=280496	JAF CMS Directory Traversal

	There is no exploit code required.	
Samba.org Samba 3.0 - 3.0.7	A buffer overflow vulnerability exists in the 'QFILEPATHINFO' request handler when constructing 'TRANSACT2_QFILEPATHINFO' responses, which could let a remote malicious user execute arbitrary code. Update available at: http://www.samba.org/samba/download/ Currently we are not aware of any exploits for this vulnerability.	Samba 'QFILEPATHINF Buffer Overflov CVE Name: CAN-2004-088
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download An exploit script is not required.	SquirrelMail Cross-Site Scripting
Thomson Speed Touch Pro ADSL	A vulnerability exists in the modem line, which could let a remote malicious user poison DNS entries via DHCP. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Thomson Spee Touch Pro ADS Remote DNS Modification
VBulletin VBulletin 3.0.1-3.0.3	An input validation vulnerability exists in 'last.php' due to insufficient validation of user-supplied input in the 'fsel' parameter, which could let a remote malicious user execute arbitrary code. *Note: The script is a 3rd party product and is not part of the vBulletin product.* No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	VBulletin 'last.ph Input Validatio
yahoopops.sourceforge.net YPOPs! 0.x	Several buffer overflow vulnerabilities exist in the POP3 and SMTP services, which could let a remote malicious user execute arbitrary code.	YPOPs! Buffe Overflows

	No workaround or patch available at time of publishing. **Another exploit script has been published.**	

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 15, 2004	NetworkMessengerDOS.pl	No	Perl script that exploits the Secure Network Messenger Remote Denial of Service vulnerability.
November 13, 2004	101_netn.cpp	No	Script that exploits the AlShare Software NetNote Server Remote Denial of Service vulnerability.
November 13, 2004	CCProxy_exp.c	Yes	Script that exploits the CCProxy HTTP Request Processing Buffer Overflow vulnerability.
November 13, 2004	grams.html	N/A	Full analysis of the

			Win32.Grams trojan.
November 13, 2004	IMail-8.13-DELETE.pm	No	Exploit script for the Ipswitch IMail Server Delete Command Remote Buffer Overflow vulnerability.
November 13, 2004	lkbackdoor.tar.gz	N/A	Paper that describes how to add a quick backdoor into the setuid code for the Linux 2.4 kernel series.
November 13, 2004	netnote_exp.c	No	Script that exploits the AlShare Software NetNote Server Remote Denial of Service vulnerability.
November 13, 2004	Shadow_Software_Attack.pdf	N/A	Whitepaper written to demonstrate that a shadow software attack is still possible.
November 13, 2004	technote.pl	No	Exploit for the Technote 'main.cgi' Input Validation vulnerability.
November 13, 2004	waraxe-2004-SA037.txt	Yes	Proof of Concept exploit for the Phorum 'follow.php' Input Validation vulnerability.
November 12, 2004	101_slim.cpp	No	Script that exploits the WhitSoft Development SlimFTPd

			Remote Buffer Overflow vulnerability.
November 12, 2004	binfmt_elf.txt	Yes	Script that exploits the Linux Kernel BINFMT_ELF Loader vulnerability.
November 12, 2004	HOD-kerio-firewall-DoS-expl.c	Yes	Script that exploits the Kerio Personal Firewall IP Options Denial of Service vulnerability.
November 12, 2004	pop_exp2.py	No	Script that exploits the YPOPs! Buffer Overflows vulnerability.
November 12, 2004	Scan6.zip	N/A	Port scanner for Windows 2k/XP that is functional for both IPv4 and IPv6 networks. Binary, source code, and more information included in the archive.
November 12, 2004	status.htm xcellent.html	No	Exploits for the Microsoft Internet Explorer Flash Content Status Bar Spoofing Weakness vulnerability
November 11, 2004	binfmt_elf_dump.c	Yes	Script that exploits the Linux Kernel BINFMT_ELF Loader vulnerability.
November 10, 2004	101_mini.cpp	No	Exploit for the MiniShare

			Buffer Overflow vulnerability.
November 10, 2004	slimFTPDCommandBObyclass101.c	No	Script that exploits the WhitSoft Development SlimFTPd Remote Buffer Overflow vulnerability.
November 8, 2004	IEnumerate.txt	No	Exploit for the Microsoft Internet Explorer 'res:' URI Handler File Identification vulnerability.

[back to top]

Trends

- Security events in the third quarter jumped 150 percent over the same period last year, fueled by more sophisticated hackers writing better code who are more interested in dollars than creating computer disasters, said Internet security firm VeriSign Tuesday. For more information, see http://www.verisign.com/static/017574.pdf.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date

1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Netsky-B	Win32 Worm	Stable	February 2004
7	Netsky-Q	Win32 Worm	Stable	March 2004
8	Bagle-Z	Win32 Worm	Stable	April 2004
9	Bagle.AT	Win32 Worm	Stable	October 2004
10	Netsky-C	Win32 Worm	Stable	February 2004
10	Bagle-AI	Win32 Worm	Stable	July 2004

Viruses or Trojans Considered to be a High Level of Threat

- Troj/Banker-AJ: Security experts have issued a red alert over a previously undocumented Trojan designed to help criminals break into the accounts of UK internet banking customers. The Banker-AJ Trojan (Troj/Banker-AJ) targets users of online banks including Abbey, Barclays, Egg, HSBC, Lloyds TSB, Nationwide, and NatWest, according to security firm Sophos. Banker-AJ has been coded to lie dormant in the background on infected Windows PCs, waiting for users to visit legitimate online banking websites. Once the user visits one of a number of banking websites the malicious code is triggered into action, capturing passwords and taking screenshots. This information is then relayed to remote hackers who can use it to break into the bank accounts of innocent users and steal money, (Vnunet.com, November 11, 2004).
- Large numbers of Bofra.E@mm and Mydoom.AK@mm worm infections are being reported. They exploit the malformed IFRAME Remote Buffer Overflow Vulnerability in Microsoft Internet Explorer. For more information on this vulnerability see US-CERT Vulnerability Note VU#842160.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Agobot-NX		Internet Worm
Backdoor.Curdeal		Trojan
Backdoor.Selka		Trojan

Downloader-SH		Trojan
Prutec		Trojan
StartPage-FJ		Trojan
Theug.B	W32/Theug.B.worm	Win32 Worm
Troj/Banker-AJ	BackDoor-CHN.gen PWSteal.Revcuss.A Trojan-Spy.Win32.Banker.ey W32/Sillydl.LZ@dl Win32.Revcuss.H Win32/PWS.Banker.AJ.Trojan	Trojan: Password Stealer
Troj/Banker-FA	Trojan-Spy.Win32.Banker.fa PWS-Bancban.gen.b	Trojan
Troj/Krepper-L	Trojan.Win32.Krepper.ab	Trojan
Troj/Mastseq-H		Trojan
TROJ_DELF.HA	Spam-SMS.Vlasof Troj/Delf-HA TrojanDownloader.Win32.Delf.fd	Trojan
TROJ_VIDLO.G	Trojan-Downloader.Win32.Vidlo.g Downloader-sg;Troj/Vidlo-G TROJ_DLOADER.S	Trojan
Trojan.Beagooz.D		Trojan
Trojan.Minuka		Trojan
Trojan.Moo.B		Trojan
Trojan.Webus.D		Trojan
Vundo.dldr		Trojan
W32.Beagle.AX@mm		Win32 Worm
W32.Envid.A@mm		Win32 Virus
W32.Mydoom.AK@mm		Win32 Worm
W32.Scard	BackDoor-CJV W32/Aler.A.worm Worm.Win32.Aler WORM_GOLTEN.A W32/Golten.worm	Win32 Worm
W32/Beagooz		Win32 Worm
W32/Bofra-D	Worm/MyDoom.AH I-Worm.Bofra.b W32/Mydoom.gen@MM Worm.Mydoom.AD	Win32 Worm
W32/Bofra-E	W32/Mydoom.gen@MM I-Worm.Bofra.c W32.Bofra.E W32.Bofra.E@mm	Win32 Worm
W32/Bofra-G	I-Worm.Bofra.b	Win32 Worm

	W32/Bofra-D W32/Mydoom.ah@MM W32/Mydoom.gen@MM Win32.Bofra.G Win32.Bofra.H Win32.Mydoom.AJ Win32.Mydoom.AL Win32/Mydoom.AF Win32/Mydoom.AJ.Worm Win32/Mydoom.AL.Worm	
W32/Cran.worm.a		Win32 Worm
W32/Forbot-CI	WORM_WOOTBOT.CJ	Win32 Worm
W32/Forbot-CJ	Backdoor.Win32.Wootbot	Win32 Worm
W32/Protoride-W		Win32 Worm
W32/Rbot-PH		Win32 Worm
W32/Rbot-PJ		Win32 Worm
W32/Rbot-PS		Win32 Worm
W32/Rbot-PU	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.p	Win32 Worm
W32/Ssik-A	WORM_SSIK.A	Win32 Worm

[back to top]

Last updated November 17, 2004